# Port knocking

Port-knocking the a obfuscation-as-security technique. It basically means that after knocking on ports in a specific sequence a certain port will open automatically. It seems to be more popular in Capture-the-flag contests than real life networks. But I have included it anyways, since CTF:s are great.

This is a way to hide certain ports, so you don't get unwanted intrusion-intents.

So for example, imagine you access your server through `ssh`. But you are tired of getting unwanted bruteforce attempts all day long. You can just have the SSH-port closed and when you knock on certain ports in a specific order the ssh-port opens up, maybe for a few minutes, or maybe indefinitely until you close it again.

When you "knock" on a port you are really just sending TCP-packets with `SYN`-flag to that port. The closed port will then respond with a `ACK/RST`. Which basically means that the host has received the `TCP`-packet, and it ACKnolwdge it, but responds with a Reset (`RST`) flag. `RST` just means that the port is closed.

## Software to implement port-knocking

I have seen the Knock software implemented.

## Opening

So, how do we actually knock? As mentioned before a knock is essentially just sending a packet to a specific port. I guess there are quite a few ways to do this. But here are three ways.

1. Knock
    - `apt-get install knockd`
    - Then you simply type: `knock [ip] [port]`. For example: `knock 192.168.1.102 4000 5000 6000`
    - After that you have to scan the network to see if any new port is open.
    - If you know what port is open you can connect to the port using netcat. The following command would work `nc 192.168.1.102 8888`. This would then connect to the port.
2. Nmap/bash

- `for x in 4000 5000 6000; do nmap -Pn --host_timeout 201 --max-retries 0 -p $x server_ip_address; done` 3. Netcat

```
nc 192.168.1.102 4000
nc 192.168.1.102 5000
nc 192.168.1.102 6000
nc 192.168.1.102 8888
```

## Break it

One way hack a server with port-knocking implemented would be to sniff for packets on the network. So if you are on the same network and able to make MITM, you can just sniff that traffic and then find the sequence.

## Pitfalls

Using port-knocking as a way to secure your service might come with some risk. The biggest risk I suppose is that if the knock-daemon fails, for whatever reason. You will be shut out of you machine. There are of course ways to just restart the knock-daemon if it fails. But maybe that daemon fails as well.

### References

This wikipedia-article is really worth reading. https://en.wikipedia.org/wiki/Port_knocking